

In re Patent Application of:
WUIDART
Serial No. 10/606,161
Filing Date: JUNE 25, 2003
_____ /

REMARKS

Applicant would like to thank the Examiner for the thorough examination of the present application, and for allowing Claims 11-22. The dependency of Claim 31 has been changed to correct the informality as helpfully noted by the Examiner. Applicant would also like to thank the Examiner for correctly indicating as allowable the subject matter of dependent Claims 2-4, 8-9, 25-27 and 30-31.

Independent Claims 1 and 23 have been amended to more clearly define the present invention over the cited prior art references. In addition, dependent Claims 2 and 24 have also been amended. Certain dependent claims have also been amended for consistency. The claim amendments and arguments supporting patentability of the claims are provided below.

I. The Amended Claims

The present invention, as recited in amended independent Claim 1, for example, is directed to a logic circuit for performing a logic function, and having N data inputs and M data outputs, with N being at least equal to 2 and M being at least equal to 1. The logic circuit comprises different logic gates or different transistors for performing the logic function in at least two different ways corresponding to different data paths or different electrical paths through the different logic gates or different transistors. The way in which the logic function is performed is based upon a value of a selection signal such that for identical data received at the N data inputs and for different values of the selection signal. At least one of

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

polarities of certain internal nodes of the logic circuit are not identical, and current consumption of the logic circuit is not identical.

The logic circuit advantageously combats piracy to improve the security of secured integrated circuits by scrambling its internal operations. Independent Claim 23 has been amended similar to amended independent Claim 1, and is directed to a method for scrambling operation of a logic circuit that performs a logic function as defined above.

II. The Claims Are Patentable Over Ohki Et Al.

The Examiner rejected independent Claims 1 and 23 over the Ohki et al. patent. The Ohki et al. patent is directed to reducing the correlation or dependency between data processing and its current consumption of an IC card.

The IC card has a storage memory including a program storage unit for storing a program, and a data storage unit for storing data. A central processing unit executes a predetermined process in accordance with a program to process the data. The program includes one or more data process units each having a process instruction for giving an execution instruction to the central processing unit. A data process order is randomly exchanged and a dummy process is added to thereby reduce the dependency of consumption current of an IC chip during the data process.

The Applicant respectfully submits that the Examiner has mischaracterized the Ohki et al. patent. Like the claimed invention, the Ohki et al. patent relates to anti-DPA methods,

In re Patent Application of:
WUIDART
Serial No. 10/606,161
Filing Date: JUNE 25, 2003

i.e., methods for de-correlating the current consumption corresponding to the logic functions used in the process being performed. Reference is directed to column 2, line 55 to column 3, line 45 in the Ohki et al. patent for the disclosed methods for scrambling the current consumption. These methods are summarized as follows.

One method of reducing the dependency of consumption current of an IC chip upon data process is when normal input data and its bit inverted data are processed. By using the normal input data and its bit inverted data by the same instruction, the number of transitions of the data on a data bus, from "0" to "1" or vice versa, can be made constant. The data transition on the data bus consumes a large amount of current. By making the number of transitions on the data bus constant, the number of current consumptions is made constant so that the dependency of consumption current upon data process can be reduced.

An alternative method of processing normal data and bit inverted data in the same manner includes providing a routine of processing the bit inverted data by an instruction that is same as the normal instruction if the same routine cannot process both the normal data and bit inverted data. Normal input data and bit inverted data are always generated for the data once processed in order to process the normal data and bit inverted data in the same manner.

Yet another method of reducing the dependency of consumption current upon data process is based on if there are a number of repetitive processes as many as there are data sets to be processed. The data is not processed in the predetermined

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

order, but the process order is changed randomly.

Another method is to add a dummy process which does not influence the corresponding process of a program, so that the operation of the equipment being executed at which place cannot be known. A combination of dummy processes and random execution of repetitive processes is effective for reducing the dependency of consumption current upon data process.

Use of both the normal data and bit inverted data, and a combination of dummy processes and random execution of repetitive processes is particularly effective for reducing the dependency of consumption current upon data process during a data permutation process and data substitution process on a byte-unit basis.

Cryptosystems such as DES (data encryption standard) use many exclusive logical OR operations. Therefore, an exclusive logical OR unit for performing an exclusive logical OR of input data and cipher key data and a bit inverted exclusive logical OR unit for performing an exclusive logical OR of bit inverted input data and cipher key data are effective for reducing the dependency of consumption current upon data process. A nonlinear substitution process unit for nonlinearly substituting input data and generating a substitution result and bit inverted substitution result and a nonlinear substitution process unit for nonlinearly substituting input bit inverted data and generating a substitution result and bit inverted substitution result are effective for reducing the dependency of consumption current upon data process. A nonlinear permutation process unit for nonlinearly permuting input data and generating a permutation

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

result and bit inverted permutation result and a nonlinear permutation process unit for nonlinearly permuting input bit inverted data and generating a permutation result and bit inverted permutation result are effective for reducing the dependency of consumption current upon the data process.

To summarize, the Ohki et al. patent teaches the following methods and combinations thereof for reducing the dependency of consumption current of an IC chip upon data process:

- Process normal input data and its bit inverted data;
- Provide a routine of processing the bit inverted data by an instruction same as the normal instruction (if the same routine cannot process both the normal data and bit inverted data);
- The data is not processed in the predetermined order but the process order is changed randomly;
- Provide a dummy process which does not influence the corresponding process of a program; and
- In cryptosystems such as DES, provide a nonlinear substitution process unit for nonlinearly substituting input data and generating a substitution result and bit inverted substitution result and a nonlinear substitution process unit for nonlinearly substituting input bit inverted data and generating a substitution result and bit inverted substitution result.

These methods are based on a specific manipulation of data or on a scrambling of the order in which steps of data processing are performed. None of these methods disclose performing the same logic function in at least two different ways

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

corresponding to different data paths or different electrical paths through different logic gates or different transistors as recited in amended independent Claim 1.

Reference is now directed to column 6, lines 41-60 of the Ohki et al. patent, which provides:

"Referring to FIG. 3, DES cryptography will be described. A cipher text is subjected first to initial permutation (IP) 301. This permutation is performed by using an initial permutation table to exchange 64-bit data of the cipher text on the one-bit unit basis. A series of such operations is repeated sixteen stages to inverse permutation (IP.sup.-1) 313 of the initial permutation."

"At each stage, a process called a f function 303 is calculated by inputting data of 32 bits of either the first or second half at the preceding stage and the cipher key, and then an exclusive logical OR operation 305 is performed by using the output of the f function and 32 bits of the remaining half at the preceding state. Data of the cipher key is also exchanged. Data of the cipher key is first subjected to selectable permutation PC-1 (302) by using a table PC-1. Thereafter, data of the cipher key is subjected to selectable permutation PC-2 (304) by using a table PC-2. At the next stage, each set of 28 bits of the cipher key rounded in accordance with an RS table is used."

This merely describes a permutation of data used during the classical steps of the DES algorithm and not a permutation of

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

data paths of electrical paths through which the discrete logic functions involved in the DES algorithm are performed. Reference is now also directed to column 7, line 58 to column 8, line 17 of the Ohki et al. patent, which provides:

"The procedure of the selectable permutation is illustrated in FIG. 24."

"The selectable permutation process processes input 32-bit data on a 6-bit unit basis and generates data of 48 bits. The data to be processed includes input normal data and its bit inverted data, and is constituted of two bytes each having 8 bits. The selectable permutation process is generally executed in the arrangement order of the E selectable permutation matrix. However, in this case, since the data process order is always constant, data to be processed may be presumed. In this embodiment, therefore, the execution order is randomized and a dummy process is added randomly so as not to make the execution order constant. With a randomized execution order, the dependency of consumption current upon data process can be reduced."

"In the selectable permutation process of this embodiment, execution flags are cleared (2402). This execution flag takes a value "1" if a corresponding bit in each process repetition unit has been processed completely, whereas it take a value "0" if it is not still processed. If all bits of the execution flags are "1", the process is terminated, whereas if not, the process continues to acquire a random number (2404). If the IC card chip has a random

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

number generator, the random number may be supplied from the generator.

Alternatively, a pseudo random number may be generated in a software way (refer to "Introduction of Cryptography Theory" by Eiji Okamoto, KYOURITSU Publishing Co., at pp. 61-86)."

Reference is also directed to column 8, lines 42-65 of the Ohki et al. patent, which provides:

"Next, the execution flag corresponding to a bit processed is set to "1" (2406). One means for achieving this is the following method. Namely, in the following formula (3), the execution index corresponding to the processed bit is set to "1", and in the following formula (4), an exclusive logical OR between the execution index and execution flag is calculated to set the execution flag of the processed bit to "1". With the above processes, the process repetition unit is selected randomly by using a random number so that the order of process repetition units does not become constant."

"Accordingly, the dependency of consumption current upon data process does not appear and a presumption of data process and cipher key becomes difficult. Since the process repetition unit is selected and executed randomly, there is a possibility that the same process is executed twice or more. This makes the process time indefinite so that a presumption of the dependency of consumption current upon data process becomes more difficult."

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

In the above mentioned paragraphs, the Ohki et al. patent thus discloses the following different methods:

- Process normal data and its bit inverted data;
- Change process order randomly;
- Provide a dummy process; and
- Provide a nonlinear substitution process unit for nonlinearly substituting data.

Permuting the steps of data processing involved in the DES algorithm is not equivalent to permuting the data paths or electrical paths through which these steps of data processing are performed. Even though the claimed invention also reduces the dependency of consumption current upon data process, it does not act at the data level, but at the electrical or logical level.

Accordingly, it is submitted that amended independent Claim 1 is patentable over the Ohki et al. patent. Amended independent Claim 23 is similar to amended independent Claim 1. Therefore, it is submitted that independent Claim 23 is also patentable over the Ohki et al. patent.

In view of the patentability of amended independent Claims 1 and 23, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

**III. Amended Independent Claim 1 Is Patentable Over The Spec
Sheet Titled MC14001B Series, B-Suffix Series CMOS Gates**

The Examiner rejected independent Claim 1 over the spec sheet titled "Article MC14001B Series, B-Suffix Series CMOS Gates." The Applicant respectfully submits that the Examiner has mischaracterized this spec sheet.

The Examiner seems to confuse the idea of performing two different functions with the same logic circuit, and the idea of performing the same logic function in different ways with the same logic circuit. MC14025B is merely a chip having three NOR gates and their respective inputs and outputs.

Referring now to the table provided by the Examiner in the Official Action, the Examiner merely proves that two different logic functions can be implemented with a logic gate having several inputs if one input is used as a selection input.

However the claimed invention is not implemented in this example. In effect, the subject-matter of claim 1 is a logic circuit capable of performing the same logic function in at least two different ways corresponding to different data paths or different electrical paths through the different logic gates or the different transistors, the way in which the same logic function is performed is based upon a value of a selection signal. It can be seen that the three-input NOR gates performs two different logic functions according to the value of Pin1 as a selection signal, and not the same logic function. For example when Pin2 Pin3=00, the output is 1 if Pin1=0 and 0 if Pin1=1. Generally speaking, the claimed invention cannot be reproduced with a single gate (a NOR or other gate).

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

In conclusion, it appears that the Examiner has characterized the claimed invention as merely relating to a logic circuit capable of performing two different logic functions according to the value of a function selection signal.

Instead, amended independent Claim 1 is directed to different logic gates or different transistors for performing the same logic function in at least two different ways corresponding to different data paths or different electrical paths through the different logic gates or different transistors, with the way in which the logic function is performed being based upon a value of a selection signal such. Accordingly, it is submitted that amended independent Claim 1 is patentable over the spec sheet titled "Article MC14001B Series, B-Suffix Series CMOS Gates."

IV. Amended Independent Claim 1 Is Patentable Over The Spec Sheet Titled Quad 2-Line To 1-Line Data Selectors/Multiplexers

The Examiner rejected independent Claim 1 over the spec sheet titled "Quad 2-Line to 1-Line Data Selectors/Multiplexers." This reference merely describes a multiplexer having - like any multiplexer - a select input. The table given by the Examiner in the Office Action shows that two different logic functions are performed according to the value of the SELECT signal, for example when A=B=1.

Thus, the line data selector/multiplexer described in this document is not capable of performing the same logic function in at least two different ways according to the value of the selection signal QED. Again, it appears that the Examiner has characterized the claimed invention as relating to a logic

In re Patent Application of:
WUIDART
Serial No. 10/606,161
Filing Date: JUNE 25, 2003
_____ /

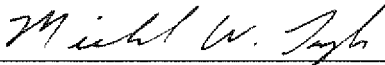
circuit capable of performing two different logic functions according to the value of a selection signal.

Instead, amended independent Claim 1 is directed to different logic gates or different transistors for performing the same logic function in at least two different ways corresponding to different data paths or different electrical paths through the different logic gates or different transistors, with the way in which the logic function is performed being based upon a value of the selection signal. Accordingly, it is submitted that amended independent Claim 1 is patentable over the spec sheet titled "Quad 2-Line to 1-Line Data Selectors/Multiplexers."

V. CONCLUSION

In view of the amendments to the claims and the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401

In re Patent Application of:

WUIDART

Serial No. 10/606,161

Filing Date: JUNE 25, 2003

Post Office Box 3791
Orlando, Florida 32802
407-841-2330